We know that every dollar in lost revenue must be made up somewhere else in the budget. And far too often, my Republican colleagues have sought to do this by reducing spending in critically important domestic spending programs such as infrastructure development, education, social security, and increased healthcare access.

As Members of Congress, it is our responsibility to pass sensible and pragmatic legislation that not only aids industry, but also grows the paychecks of hard-working families and invests in the future of our children. We must weigh this tax extenders package against its long-term impact on Congress' ability to help businesses create jobs and opportunities, grow our economy, invest in our aging infrastructure, strengthen our national security, and provide our senior citizens with the opportunity to retire with dignity. The American people deserve a more balanced bill that offsets its cost, and helps both individuals and businesses equitably across the board.

I urge my colleagues to review this legislation carefully, with a focus on our nation's future.

A NEW APPROACH TO CYBERSECURITY

HON. RICK W. ALLEN

OF GEORGIA

IN THE HOUSE OF REPRESENTATIVES

Thursday, December 17, 2015

Mr. ALLEN. Mr. Speaker, I rise to speak about an effort by Unisys, a global technology company with a presence in my district, aimed at significantly lowering the cyber risks being faced by our citizens and our government. Cyber-attacks are increasing and leaders in government and industry are seeking new approaches to protect critical data. One new approach to security, micro-segmentation, was described in detail by Unisys Vice President Tom Patterson at the 2nd Annual Cyber Education Summit held at Augusta University on October 14–15, 2015. I would like to submit a short excerpt of Mr. Patterson's remarks as it outlines the core of this important initiative.

Our original approach to cybersecurity is no longer working. Recently, we have watched as companies, governments, and institutions report system breaches on a nearly weekly basis. It is clear that core assumptions and approaches that defined our old security models are failing.

We rely on computing and communications systems that are critical to our financial systems, health care providers, schools, governments, and business enterprises. It's not just our computers that are at risk. Increasingly, cyber-attacks jeopardize careers, wallets, companies, infrastructure, and even lives. Adversaries boldly wield the power to access personal and corporate data online and take control of systems throughout our interconnected world.

A fresh approach to security is needed. The new approach must account for our modern infrastructure—employees work from home, users need access to information on mobile devices, and supply chains are integrated and interdependent. The new approach should also accommodate changes in the adversaries. Attackers are both more skilled and more motivated. New cybersecurity systems need to assume that infiltrations will occur and must provide tools to localize and limit the damage.

At the core of this new approach is micro-segmentation. If segmentation is analogous to a bank vault, micro-segmentation is akin to the many safe deposit boxes within the vault.

Micro-segmentation is much more secure and inclusive, and easier to implement and manage. It embraces new technologies like clouds, and new business models like integrated supply chains. It delivers real results that are cost-effective and resource efficient.

Micro-segmentation allows enterprise managers to divide physical networks quickly and easily into hundreds or thousands of logical micro networks, or microsegments. Setting up microsegments keeps the different parts of an organization logically separate, thus lowering the intrusion risk. If a breach happens, the intruder can only see one segment.

Micro-segmentation works at the Internet packet level, cryptographically sealing each packet so that only packets within the approved microsegment are processed.

For every packet, the data is completely encrypted, and the routing information in the headers is cryptographically sealed to ensure only authorized delivery. Users can only send and receive packets for a specified group.

Micro-segmentation is implemented by software, and it therefore operates independent of any given network topology or network hardware. Organizations have a single security model that works equally well in local data centers and the public cloud. With micro-segmentation, organizations can extend security to the cloud while retaining control of data in motion and the keys that secure it. Micro-segmentation enables access to the benefits of the cloud—cost savings and network flexibility—without sacrificing security. Micro-segmentation can be quickly and easily implemented within virtual machines to defend against side-channel attacks and other risks that are specific to cloud architectures.

Micro-segmentation makes it easier to integrate component suppliers by providing just the right amount of access. Micro-segmentation can also protect legacy systems, allowing organizations to use older operating systems while keeping them isolated from newer systems.

By embracing a new approach to cybersecurity, we can dramatically increase the strength of our networks and confront the new threat with new tools.